International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 4, Aug 2014, 69-76
© TJPRC Pvt. Ltd.

A NEW APPROACH OF MULTIAGENT AND MULTILEVEL IDS

ARPITA BISWAS & MEENAKSHI SHARMA

Department of Computer Science and Engineering, SSCET, Badhani, Punjab, India

ABSTRACT

In daily life network is an important issue and now a day's network is a part of our life. We use networking system for all types of work. We store our personal information, data in the network. But this network system is increasing day by day and it is difficult to manage this networking system. For that there is introduced Intrusion Detection System. It is a system by which we detect Intrusion. It detects any malicious behavior, vulnerabilities of the system. In this paper multilevel attached with Multiagent intrusion detection system is proposed.

KEYWORDS: Multiagent, Multilevel, Encryption, Decryption

INTRODUCTION

In this world many attacks done through the network. So we should need to provide steps against this attack types. We secure the network system by the firewall, vulnerability check and encryption process, but the attacker's are very intelligent and they take advantage of any defect or social engineering site. There are two types of attacks present. Insider attack and outsider attack [1] insider attacks means legitimate user, who have power to access the information, leaks this information. For an example in on large organization if an employee who have the power to access the companies personal information is upset with this company for any reason then this employee leaks the companies information to the outside. This is called insider attack. In the outsider attack here the attacker attack from the outside. The attacker uses any of the defect or vulnerability and access the information. That's why introduced Intrusion Detection System. By this system attack types are detected and generate an alarm to the administrator and immediately take an action by the administrator.

The concept of Intrusion detection system was first introduced by Anderson to complement conventional computer security approaches in 1980 [1]. To improves the existing intrusion detection system this paper introduces multilevel attached with Multiagent intrusion detection system. When information are send from one server to another then before receiving this information it is checked by the proposed Intrusion Detection architecture. Where information checked through different level that's why we get more secure information and here the total information is divided into different agent who works together and completes the whole task. In this process less time is needed.

INTRUSION DETECTION SYSTEM

Intrusion means break the normal behavior of the system. Intrusion Detection System means detection of the malicious behavior or vulnerability. There have present different types of IDS:

HIDS: Host based Intrusion Detection System. Here Intrusion is detected only in one single host. All the traffics of single host are monitor and if attacks detected then generate an alarm.

NIDS: Network based Intrusion Detection System. Here intrusion is detected only in one network between client and server. But in the NIDS if encrypted information is passed then it is not able to detect intrusion from this information.

DIDS: Distributed Intrusion Detection System. Here intrusion is detected in the distributed network between the servers.

Three have also present different types of model which detect intrusion. These types are:

Abnormality Check Process: It is a one type of Intrusion Detection Process by which intrusion is detected easily. It is based on the normal and abnormal behavior. When we check one information flow and if one behavior is changed or abnormal behavior is found then it is called attack means if the behavior is deviate from the normal it is called intrusion. Here information are collected from the open network and when use the abnormality check process here match the exact behavior from this collected information, if it is not matched then we called this is intrusion.

Misuse Detection Process: It is one Intrusion Detection Process by which only known attack types are detected. Here maintain one database where the attack types or pattern are stored from the open network or any sequence of action. When information is checked by this process we matched only known patterns or sequence and discover the results.

MULTIAGENT TECHNIQUE

Multiagent means more than one agent work together and complete task and also use same resource [1, 2, 4] in this paper three types of agents are used. This agents divide the task among them and work individually for same goal. They work independently and not interfere in one another’s work.

MULTILEVEL TECHNIQUE

Multilevel means intrusion is detected in different level [2].1st of all here information is encrypted and divided among the agent. Agent sends this information. Before receiving the information receiver decrypt the information and matched the integrity. If it is not matched then generates an alarm to the administrator about intrusion and stops the work otherwise it sends the information to the next level where an apriori algorithm is used [5, 6]. By this algorithm the information are checked 2nd time and we get the better result.

RELATED WORK

Intrusion Detection System is introduced to protect the computer network system. To improve the intrusion detection system here used Multiagent technique [1, 2, 3, 4] by this technique multiple agents work together and complete one task. Less time is needed to detect intrusion by Multiagent. By the Multilevel technique also the information is checked in different level [2, 4] and we get the better solution. We use encryption and decryption [7] to improve the security level of the system. In this paper use apriori algorithm to detect intrusion by using association rules [5,6].

PROPOSED WORK

In this paper we proposed the improve technique of Intrusion Detection System. In this paper Multiagent and multilevel techniques work together for better result. In this proposed work when one sender sends a message then encryption [7] is done and then divides this message among the three agents. Now send the message. Before receives this message 1st decrypt this message and matched its integrity. If there is found any malicious activity then it generates an alarm to the administrator. Because of an encrypted message agents are not also able to done any type of distortion with this message. Now if no intrusion is detected in this level then this information is passed through the next level. In this level apriori algorithm [5, 6] is used to check the information and detect intrusion. In this algorithm find the frequent item set and by this item set make an association rule which is used to detect intrusion. If intrusion is detected then generates an alarm to the administrator and stops the work otherwise it stores the information as a normal and show the message to the receiver. Figure 1 describes the working process of the proposed Intrusion Detection System.

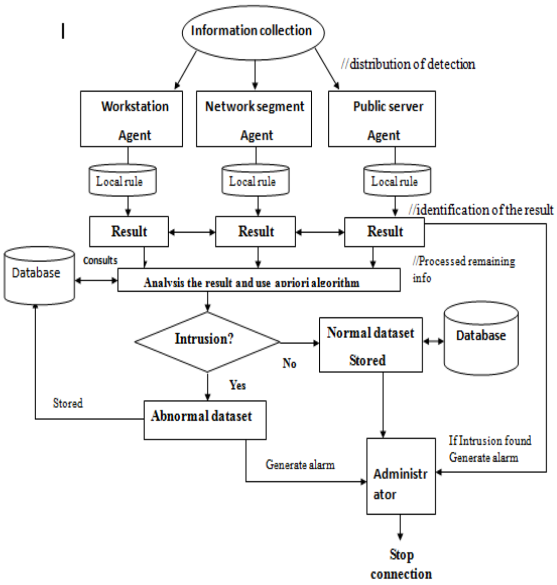


Figure 1: Architecture of Propose System

Algorithm Used by Agents: 1st Level: In this level agent use their own rule. Which describe bellow:

Encryption Process of the File

- User prepares a message for sending.
- User calculates the size of the received message.
- User than calculates the hashes of the received message. This hash values will be used for integrity checking. Any changes in the data will change the hash value of the same file.
- User then encrypts the Message and sends the encrypted message to the server.

Decrypt Process of the File

- Server first requests for the intended message and key.
- User sends the key.
- Sever decrypts the message.
- Here for integrity verification Server performs the following tasks:

- o Server first calculates the size of the received message. If the file size is matched with the previously stored one, then Server performs (ii). Else the integrity of the message has been lost.
- o Server calculates the hash of the received message and matches it with the stored one. If it matches then the message is ok, else its integrity has been lost.

- After verification Server sends the data to next level if its integrity is not lost.
- Server decrypts the message with the same password as provided by the user.

Algorithm: 2nd Level: In the 2nd level agent use another [5] [6] algorithm to detect the intrusion from the remaining information. The algorithm used by the agents mentioned bellow:

- Size of the information N
- If frequent item set F_N= null, algorithm begin
- F_N generates C_{N+1}(candidate count)
- Increments the count of all frequent items set in database.
- $C_{N+1}=F_N$ join F_N
- C_N+K= null, terminate the algorithm.

Let's take an example: the information collected in the database. There have 9 transactions are present. Table 1 describes the information database, Table 2 describes the candidate count for 1-item set C1, Table 3 describes the frequent item set F1, Table 4 describes the count of 2 item set C2, Table 5 describes the frequent item set F2, Table 6 describes the count of 2 item set C3, Table 7 describes the frequent item set F3, Table 8 describes the count of 2 item set C4

Table 1: Information Database

Transaction ID	Data Item Set
T1	I2,I4,I1
T2	I2,I4
T3	I5,I3
T4	I2,I4,I3
T5	I2,I5
T6	I4,I3
T7	I2,I3
T8	I2,I4,I1,I3
T9	I2,I4,I1

Count of each candidate for 1item set frequent pattern:

- We find the count of each candidate from database which is C1.
- Then compare this count with the minimum count of each candidate which is called frequent item set F1.

Table 2: C1 Database

Data Item Set	Count in Database
I1	3
I2	7
I3	5
I4	6
I5	2

Table 3: F1 Database

Data Item Set	Count in Database
I1	3
I2	7
I3	5
I4	6
I5	2

Count of candidate for 2-item set frequent pattern:

- Find count of candidate item set C2 by the join operation of F1.
- Find frequent item set F2 from the C2.

Table 4: C2 Database

Data Item Set	Count in Database
I1,I2	3
I1,I3	1
I1,I4	3
I1,I5	0
I2,I3	3
I2,I4	5
I2,I5	1
I3,I4	3
I3,I5	1
I4,I5	0

Table 5: F2 Database

Data Item Set	Count in Database
I1,I2	3
I1,I4	3
I2,I3	3
I2,I4	5
I3,I4	3

Count of candidate for 3-itemset frequent pattern:

- Find count of candidate item set C3 by the join operation of F2.
- Find frequent item set F3 from the C3.

Table 6: C3 Database

Data Item Set	Count in Database
I1,I2,I4	3
I1,I2,I3	1
I1,I4,I3	1
I2,I3,I4	2

Table 7: F3 Database

Data Item Set	Count in Database
I1,I2,I4	3
I2,I3,I4	2

Count of candidate for 4-itemset frequent pattern:

- Find count of candidate item set C4 by the join operation of F3.
- C4= null, terminate the operation.

Table 8: C4 Database

Data Item Set	Count in Database
I1, I2, I3, I4	1

Then the frequent item set: {I1}, {I2}, {I3}, {I4}, {I5}, {I1, I2}, {I1, I4}, {I2, I3}, {I2, I4}, {I3, I4}, {I1, I2, I4}, {I2, I3, I4}.

Now we make a rule from this frequent item set. Suppose min support count is 2 means 22.22%. Let minimum confidence is 75%.

So the rule is if frequent item set F then subset S → (F-S). Let's take an example:

we have frequent item set [I1], [I2], [I3], [I4], [I1,I2], [I1,I3], [I1,I5], [I2,I3], [I2,I4], [I2,I5], [I1,I2,I3], [I1,I2]

Say, F= [I1, I2, I4]

Sub set S= [I1], [I2], [I4], [I1, I2], [I1, I4], [I2, I4]

Resultant rule is:

R1: [I1] → [I1, I2, I4]-[I1] = [I2, I4]

Confidence = sc [I1, I2, I4]/sc [I1] =3/3=100%

Rule R1 is selected for rule.

R2: [I2] → [I1, I2, I4]-[I2] = [I1, I4]

Confidence = sc [I1, I2, I4]/sc [I2]=3/7=42%

Rule R1 is not used because it is below the threshold value.

R3: [I4] → [I1, I2, I4]-[I4] = [I1, I2]

Confidence = sc [I1, I2, I4]/sc [I4] = 3/6=50%

R3 is not used because it is below the threshold value.

R4: [I1, I2] → [I1, I2, I4]-[I1, I2] = [I4]

Confidence = sc [I1, I2, I4]/sc [I1, I2] = 3/3=100%

R4 is selected for rule.

R5: [I1, I4] → [I1, I2, I4]-[I1, I4] = [I2]

Confidence = sc [I1, I2, I4]/sc [I1,I4]=3/3=100%

R5 is selected for rule.

R6: [I2, I4] → [I1, I2, I4]-[I2, I4] = [I1]

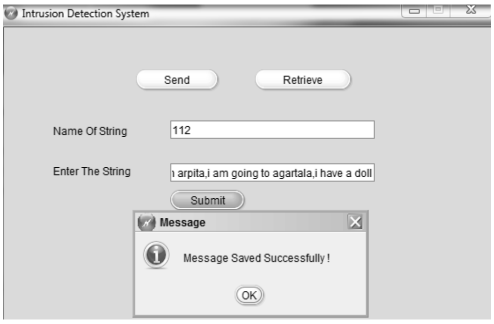
Confidence = sc [I1, I2, I4]/sc [I2, I4] = 3/5=60%

R6 is not used because it is below the threshold value.

By using this algorithm we find 4 association rules. Find the correct information and delete all unwanted, replicated things from the information.

IMPLEMENTATION RESULT AND ANALYSIS

Intrusion Detection Process: 1st of all senders send a message to the receiver shown in the Figure 2 and encrypt the message. Receiver decrypts the message shown in the Figure 3 and in the 1st level it checks the integrity of this message, if intrusion is detected then it generates an alarm to the administrator that "packet has been attacked" which is shown in the Figure 3. If integrity matches then the message go through the 2nd level and check by the apriori algorithm. After checking is completed by the two levels we get the final intrusion free result which is more secure.



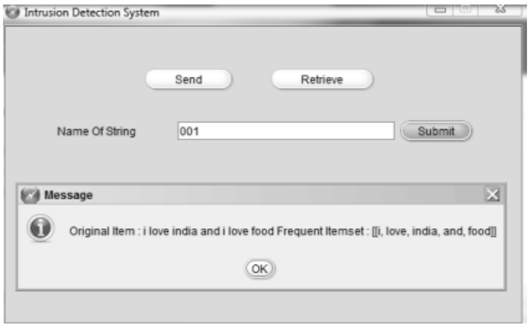
Name Of String: 112

Enter The String: ı arpita,i am going to agartala,i have a doll

Message

Message Saved Successfully !

Figure 2: Sending a Message

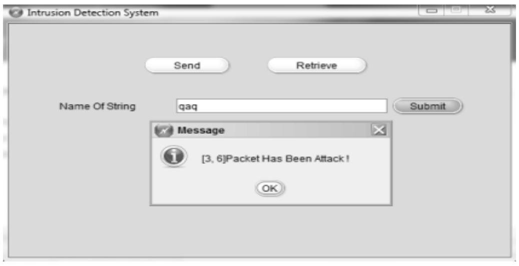


Name Of String: 001

Message

Original Item : i love india and i love food Frequent Itemset : [[i, love, india, and, food]]

Figure 3: Receiving a Message



Name Of String: qaq

[3, 6]Packet Has Been Attack !

Figure 4: Attacked Detected

CONCLUSIONS

- In this paper the Multi-agent and multilevel system work together for improving the intrusion detection system. The Multi-agent works in different level and for this the detection process results better.
- In one level it checks the integrity of the information. If there is any malicious activity presents then generate an alarm about intrusion.
- If no attracts are detected then this information is passed through the level where the information is checked 2nd time. So by this process we get the better intrusion free information.
- This approach is very helpful to us because here data is checked by different level and also less time required because the use of multi-agent. They divide their work and easily detect the intrusion. After finishing these two levels we get the final result and store it in the database.

REFERENCES

1. Ran Zhang', Depei Qian, Chongming Bao, Weiguo Wu, (IEEE 2001) *"Multiagent Based Intrusion Detection Architecture"*, pp 494-501.
2. Siham benhadou, Driss raoui Hicham medromi, *"New Methodology for Intrusion Detection based on Multi-Agents System"*,Architecture Systems team ENSEM.
3. Nita Patil,Chhaya Das, Shreya Patankar, Kshitija Pol, (IEEE 2008)*"Analysis of Distributed Intrusion Detection Systems using Mobile Agents"*,Datta Meghe College of Engineering, Airoli, Navi Mumbai- 400708, First International Conference on Emerging Trends in Engineering and Technology, pp 1255-1260.
4. Mueen Uddin, Kamran Khowaja, Azizah Abdul Rehman, (October 2010) *"Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents"*, Department of Information System,UTM, Malaysia, International Journal of Network Security and Its Applications(IJNSA), Vol.2,No.4, pp.129-141.
5. Honglie Yu, Jun Wen, Hongmei Wang,Li Jun, (Elsevier2011) *"An Improved A priori Algorithm Based On the Boolean Matrix and Hadoop"*, Advanced in Control Engineering and Information Science, pp 1828-1831.
6. Li Hanguang, Ni Yu, (Elsevier 2011) *"Intrusion Detection Technology Research Based on Apriori Algorithm"*, The School of Computer and Software Nanjing University of Information Science and Technology Nanjing, pp.1616-1620.
7. "Encryption Basics | EFF Surveillance Self-Defense Project." (06 Nov. 2013) Encryption Basics | EFF Surveillance Self-Defense Project. Surveillance Self-Defense Project, n.d. Web.